CLAIMS

1. A method of providing intrusion detection (6) in a network (2) wherein data flows are exchanged using associated network ports and application layer protocols, the method including the steps of:

- monitoring (14) data flows in said network (2),
- detecting (16) information on said application layer protocols involved in said monitored data flows; and
- providing intrusion detection (18) on said monitored data flows based on application layer protocols detected.

2. The method of claim 1, characterized in that said intrusion detection is provided independently of any predefined association between said network ports and said application layer protocols.

3. The method of claim 1, characterized in that said step of detecting (16) information on application layer protocols includes passive observation (14) of network traffic.

4. The method of claim 1, characterized in that said step of detecting (16) information on application layer protocols involves using (22) signature-matching techniques.

5. The method of claim 1, characterized in that said step of detecting (16) information on application layer protocols involved in said data flows includes the step of identifying (22, 26) at least one protocol involved in a given data flow.

6. The method of claim 1, characterized in that said step of providing intrusion detection (18) includes signature-based detection of misuse by matching at least one of a given data packet and data flow regardless of the service ports involved, based on

said information on application layer protocols.

7. The method of claim 1, characterized in that it includes providing intrusion detection (18) based on a plurality of predefined sets of analysis tasks (66) and misuse signatures (68) for a plurality of said protocols, and includes selecting out of said plurality a set related to at least one protocol involved in a given data flow and at least one of the steps of:

- performing over said data flow the selected set of analysis tasks (66), and

- performing signature matching (22) over said data flow against the selected set of misuse signatures (68).

8. The method of claim 1, characterized in that said steps of detecting information on application layer protocols (16) and providing intrusion detection (18) are performed within the same functional module and employing the same functional blocks of packet capture (19), preprocessing (20) and signature matching (22).

9. The method of claim 4, characterized in that said (22) signature-matching is performed by comparing monitored traffic with a set of (24) protocol detection signatures having the following characteristics:

- the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system, and

- each said signature specifies a respective protocol that is detected if the signature is triggered.

10. The method of claim 9, characterized in that each said signature is designed to attempt to match a pattern that is unique to a given protocol and at the same time is frequently used in said protocol.

11. The method of claim 9, characterized in that it includes the step of using at least one of signatures identifying behavior frequently present in server responses and signatures identifying common client request–server reply behavior.

12. The method of claim 9, characterized in that it involves leaving out signatures exclusively matching a pattern in client behavior.

13. The method of claim 1, characterized in that said step of detecting (16) information on application layer protocols involved in said data flows involves characterizing and classifying data flows related to each server application (10) in said network (2).

14. The method of claim 13, characterized in that said step of characterizing and classifying data flows involves monitoring features out of the group consisting of: packet size, packet arrival times, TCP flags and header information.

15. The method of claim 13, characterized in that said step of characterizing and classifying data flows involves classifying data flows and services into a number of flow classes.

16. The method of claim 13, characterized in that said step of characterizing and classifying data flows involves at least one of discriminating between interactive and non-interactive traffic and identifying specific protocols.

17. The method of claim 1, characterized in that said step of detecting information on application layer protocols (16) involved in said data flows includes producing a map (30) of associations between application layer protocols and network ports present in said network, and said step of providing intrusion detection (18) is performed on said associated network ports.

18. The method of claim 1, characterized in that said step of providing intrusion detection (18) based on said information on application layer protocols includes the steps of:

- establishing a network policy (34), and
- generating a security event whenever a protocol is detected in violation of said network policy (38).

19. A system for providing intrusion detection (6) in a network (2) wherein data flows are exchanged using associated network ports and application layer protocols, the system including:

- a monitoring module (14) configured for monitoring data flows in said network (2),
- a protocol identification engine (16) configured for detecting (16) information on application layer protocols involved in said monitored data flows; and
- an intrusion detection module (18) designed for operating on said monitored data flows based on said information on application layer protocols detected.

20. The system of claim 19, characterized in that said intrusion detection module (18) operates independently of any predefined association between said network ports and said application layer protocols.

21. The system of claim 19, characterized in that said monitoring module is a module, such as a sniffer (14), configured for passive observation (14) of network traffic.

22. The system of claim 19, characterized in that said protocol identification engine (16) includes a signature-matching feature (22).

23. The system of claim 19, characterized in that said protocol identification engine (16) is configured for detecting information on application layer protocols involved in said data flows by identifying

(22, 26) at least one protocol involved in a given data flow.

24. The system of claim 19, characterized in that said intrusion detection module (18) is configured for providing intrusion detection by signature-based detection of misuse by matching at least one of a given data packet and data flow regardless of the service ports involved, based on said information on application layer protocols.

25. The system of claim 19, characterized in that said intrusion detection module (18) is configured for providing intrusion detection based on a plurality of predefined sets of analysis tasks (66) and misuse signatures (68) for a plurality of said protocols, said intrusion detection module (18) being further configured for selecting out of said plurality a set related to at least one protocol involved in a given data flow and carrying out at least one of the steps of:

- performing over said data flow the selected set of analysis tasks (66), and

- performing signature matching (22) over said data flow against the selected set of misuse signatures (68).

26. The system of claim 19, characterized in that said protocol identification engine (16) and said intrusion detection module (18) are integrated to a common functional module and employ a common set of functional blocks of packet capture (19), preprocessing (20) and signature matching (22).

27. The system of claim 22, characterized in that the system is configured for performing said (22) signature-matching by comparing monitored traffic with a set of (24) protocol detection signatures having the following characteristics:

- the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system and

- each said signature specifies a respective protocol that is detected if the signature is triggered.

28. The system of claim 27, characterized in that each said signature is designed to attempt to match a pattern that is unique to a given protocol and at the same time is frequently used in said protocol.

29. The system of claim 27, characterized in that the system is configured for using at least one of signatures identifying behavior frequently present in server responses and signatures identifying common client request–server reply behavior.

30. The system of claim 27, characterized in that the system is configured for leaving out signatures exclusively matching a pattern in client behavior.

31. The system of claim 19, characterized in that said protocol identification engine (16) is configured for detecting (16) information on application layer protocols involved in said data flows by characterizing and classifying data flows related to each server application (10) in said network (2).

32. The system of claim 31, characterized in that said protocol identification engine (16) is configured for monitoring features out of the group consisting of: packet size, packet arrival times, TCP flags and header information.

33. The system of claim 31, characterized in that said protocol identification engine (16) is configured for characterizing and classifying data flows by classifying data flows and services into a number of flow classes.

34. The system of claim 31, characterized in that said protocol identification engine (16) is configured for characterizing and classifying data by at least one of discriminating between interactive and non-interactive traffic and identifying specific protocols.

35. The system of claim 20 characterized in that said protocol identification engine (16) is configured for producing a map (30) of associations between application layer protocols and network ports present in said network, and said intrusion detection module (18) provides intrusion detection on said associated network ports.

36. The system of claim 19, characterized in that said intrusion detection module (18) is configured for:

- establishing a network policy (34), and
- generating a security event whenever a protocol is detected in violation of said network policy (38).

37. A communication network (2) having associated a system according to any of claims 19 to 36.

38. A computer program product loadable in the memory of at least one computer and comprising software code portions for performing the steps of any of claims 1 to 18 when the product is run on a computer.